

# Networks Glossary

---

802.11a	A specification developed by the IEEE for wireless LAN (WLAN) technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. The 802.11a specification uses an orthogonal frequency division multiplexing encoding scheme rather than FHSS or DSSS and provides up to 54 Mbps in the 5GHz band.
802.11ac	A wireless LAN (WLAN) specification under development by the IEEE (Institute of Electrical and Electronics Engineers) that delivers wireless data transfer rates in the range of 433 Mbps (Megabits per second) per spatial stream. With support for up to eight streams, the 802.11ac specification offers a theoretical maximum data transfer speed of more than 3Gbps (Gigabits per second), and can deliver 1.3Gbps transfer speeds with a more common three-antenna (three streams) design.
802.11b	Also referred to as 802.11 High Rate or Wi-Fi, it is an extension to 802.11 specification developed by the IEEE for wireless LAN (WLAN) technology that applies to wireless LANS and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band. 802.11b uses only DSSS. 802.11b was a 1999 ratification to the original 802.11 standard, allowing wireless functionality comparable to Ethernet.
802.11g	An extension to 802.11 specification developed by the IEEE for wireless LAN (WLAN) technology that is used for transmission over short distances at up to 54-Mbps in the 2.4 GHz bands.
802.11n	An extension to 802.11 specification developed by the IEEE for wireless LAN (WLAN) technology. 802.11n builds upon previous 802.11 standards by adding multiple-input multiple-output (MIMO). The additional transmitter and receiver antennas allow for increased data throughput through spatial multiplexing and increased range by exploiting the spatial diversity through coding schemes like Alamouti coding. The speed is 100 Mbit/s (even 250 Mbit/s in PHY level), and so up to 4-5 times faster than 802.11g. 802.11n also offers a better operating distance than current networks.
802.11x wireless	802.11 and 802.11x refers to a family of specifications developed by the IEEE for wireless LAN (WLAN) technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. The IEEE accepted the specification in 1997.
Broadband	Operating at, responsive to, or comprising a wide band of frequencies <a broadband radio antenna> ; of, relating to, or being a high-speed communications network and especially one in which a frequency range is divided into multiple independent channels for simultaneous transmission of signals (as voice, data, or video)
Category 5 Cable	Cat 5 is a twisted pair cable for carrying signals. This type of cable is used in structured cabling for computer networks such as Ethernet. The cable standard

	provides performance of up to 100 MHz and is suitable for 10BASE-T, 100BASE-TX (Fast Ethernet), and 1000BASE-T (Gigabit Ethernet). Cat 5 is also used to carry other signals such as telephony and video.
Category 5e Cable	The category 5e specification improves upon the category 5 specification by tightening some crosstalk specifications and introducing new crosstalk specifications that were not present in the original category 5 specification. The bandwidth of category 5 and 5e is the same – 100 MHz. The differences between category 5 and category 5e are in their transmission performance. Category 5e components are most suitable for a high-speed Gigabit Ethernet. While category 5 components may function to some degree in a Gigabit Ethernet, they perform below standard during high-data transfer scenarios.
Category 6 Cable	A standardized cable for Gigabit Ethernet and other network physical layers that is backward compatible with the Category 5/5e and Category 3 cable standards. Compared with Cat 5 and Cat 5e, Cat 6 features more stringent specifications for crosstalk and system noise. The cable standard provides performance of up to 250 MHz and is suitable for 10BASE-T, 100BASE-TX (Fast Ethernet), 1000BASE-T/1000BASE-TX (Gigabit Ethernet) and 10GBASE-T (10-Gigabit Ethernet).[
Device Authentication-- MAC Address	Is used to authenticate devices based on their physical media access control (MAC) address. While not the most secure and scalable method, MAC-based authentication implicitly provides an additional layer of security authentication devices. MAC-based authentication is often used to authenticate and allow network access through certain devices while denying access to the rest. For example, if clients are allowed access to the network via station A, then one method of authenticating station A is MAC-based. Clients may be required to authenticate themselves using other methods depending on the network privileges required.
DHCP (dynamic host control protocol),	is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway. DHCP allows hosts to obtain necessary TCP/IP configuration information from a DHCP server.
DHCP Pool	Key DHCP parameters include the range or "pool" of available IP addresses, the correct subnet masks, plus network gateway and name server addresses.
DHCP Server	A computer running the DHCP Server service that holds information about available IP addresses and related configuration information as defined by the DHCP administrator and responds to requests from DHCP clients.
DNS Server	Domain Name System (or Service or Server), an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4. (from webopedia.com)
Endpoint	anything that attached to the network, including PC, laptop, tablet, phone, iPod, etc.

Ethernet	a computer network architecture consisting of various specified local-area network protocols, devices, and connection methods
Ethernet Port	An Ethernet port is an opening on computer network equipment that Ethernet cables plug into. Ethernet ports accept cables with RJ-45 connectors
Gateway	A wireless gateway routes packets from a wireless LAN to another network, wired or wireless WAN. It may be implemented as software or hardware or combination of both. Wireless gateways combine the functions of a wireless access point, a router, and often provide firewall functions as well.
Internet Service Provider (ISP)	An organization that provides services for accessing, using, or participating in the Internet. Internet service providers may be organized in various forms, such as commercial, community-owned, non-profit, or otherwise privately owned.
IP Address	a unique string of numbers separated by periods that identifies each computer using the Internet Protocol to communicate over a network.
IPv6	Internet Protocol version 6 (IPv6) is the latest version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. IPv6 is intended to replace IPv4.
Local Area Network (LAN)	A local area network (LAN) is a computer network that interconnects computers within a limited area such as a home, school, computer laboratory, or office building, using network media.
Private IP Address	A private IP address is a non-Internet facing IP address on an internal network. Private IP addresses are provided by network devices, such as routers, using network address translation (NAT).
Public IP Address	Public addresses are assigned by InterNIC and consist of class-based network IDs or blocks of CIDR-based addresses (called CIDR blocks) that are guaranteed to be globally unique to the Internet. When the public addresses are assigned, routes are programmed into the routers of the Internet so that traffic to the assigned public addresses can reach their locations. Traffic to destination public addresses are reachable on the Internet.
RADIUS server	(Remote Authentication Dial-In User Service) RADIUS is often used by Internet service providers (ISPs) to authenticate and authorize dial-up or VPN users. The standards for RADIUS are defined in RFCs 2138 and 2139. A RADIUS server receives user credentials and connection information from dial-up clients and authenticates them to the network. RADIUS can also perform accounting services, and EAP messages can be passed to a RADIUS server for authentication. EAP only needs to be installed on the RADIUS server; it's not required on the client machine.
Router	is a networking device that forwards data packets between computer networks. A router is connected to two or more data lines from different networks.
Scalability	The ability of a system, network, or process to handle a growing amount of work in a capable manner or its ability to be enlarged to accommodate that growth. For

	example, it can refer to the capability of a system to increase its total output under an increased load when resources (typically hardware) are added.
SSID	SSID is a case sensitive, 32 alphanumeric character unique identifier attached to the header of packets sent over a wireless local-area network (WLAN) that acts as a password when a mobile device tries to connect to the basic service set (BSS) -- a component of the IEEE 802.11 WLAN architecture.
Subnet mask	used to determine what subnet an IP address belongs to. An IP address has two components, the network address and the host address. For example, consider the IP address 150.215.017.009. Assuming this is part of a Class B network, the first two numbers (150.215) represent the Class B network address, and the second two numbers (017.009) identify a particular host on this network.
Switch	a network switch (also called switching hub, bridging hub, officially MAC bridge) is a computer networking device that connects devices together on a computer network, by using packet switching to receive, process and forward data to the destination device.
Transmission Control Protocol/Internet Protocol (TCP/IP)	is the suite of communications protocols used to connect hosts on the Internet. TCP/IP uses several protocols, the two main ones being TCP and IP. TCP/IP is built into the UNIX operating system and is used by the Internet, making it the de facto standard for transmitting data over networks.
Upstream Server	In computer networking, upstream server refers to a server that provides service to another server. In other words, upstream server is a server that is located higher in the hierarchy of servers.
User Authentication--Enterprise	This profile defines a means to establish one name per user that can then be used on all of the devices and software that participate in this integration profile. It greatly facilitates centralized user authentication management and provides users with the convenience and speed of a single sign-on. User authentication is a necessary step for most application and data access operations and streamlines workflow for users.
User Authentication--Local	Authentication verifies users before they are allowed access to the network and network services. The Local Authentication framework provides facilities for requesting authentication from users with specified security policies. A local user record often consists of a username, the user's full name, and the user's password.
VLAN	A VLAN has the same attributes as a physical local area network (LAN), but it allows for end stations to be grouped together more easily even if they are not on the same network switch. VLAN membership can be configured through software instead of physically relocating devices or connections.
WAN	Most networks consist of two major zones—the local area network (LAN) and the wide area network (WAN). A LAN is the internal network, whether it is a house with two computers or a high-rise office building with thousands doesn't matter. The WAN is the network outside the LAN; this is both other internal networks and the full Internet. A WAN port is the portal by which information passes back and forth

	between the LAN and the WAN.
WAN Port	(WAN Stands for Wide Area Network)Most users will find a WAN port on a network router. A common home router has one WAN port and four LAN ports. Some routers refer to them as an uplink (for the WAN port) and wired connections (for LAN ports). The WAN port takes in information from the outside network or the Internet. The information is filtered through the router's internal firewall and routing system. Then the information is sent to the proper LAN port or out over a wireless connection to a wireless source.
Wireless Access Point (AP)	is a device that allows wireless devices to connect to a wired network using Wi-Fi, or related standards. The AP usually connects to a router (via a wired network) as a standalone device, but it can also be an integral component of the router itself.